



Web App Testing Methodology & Web App Components

About The Presenter

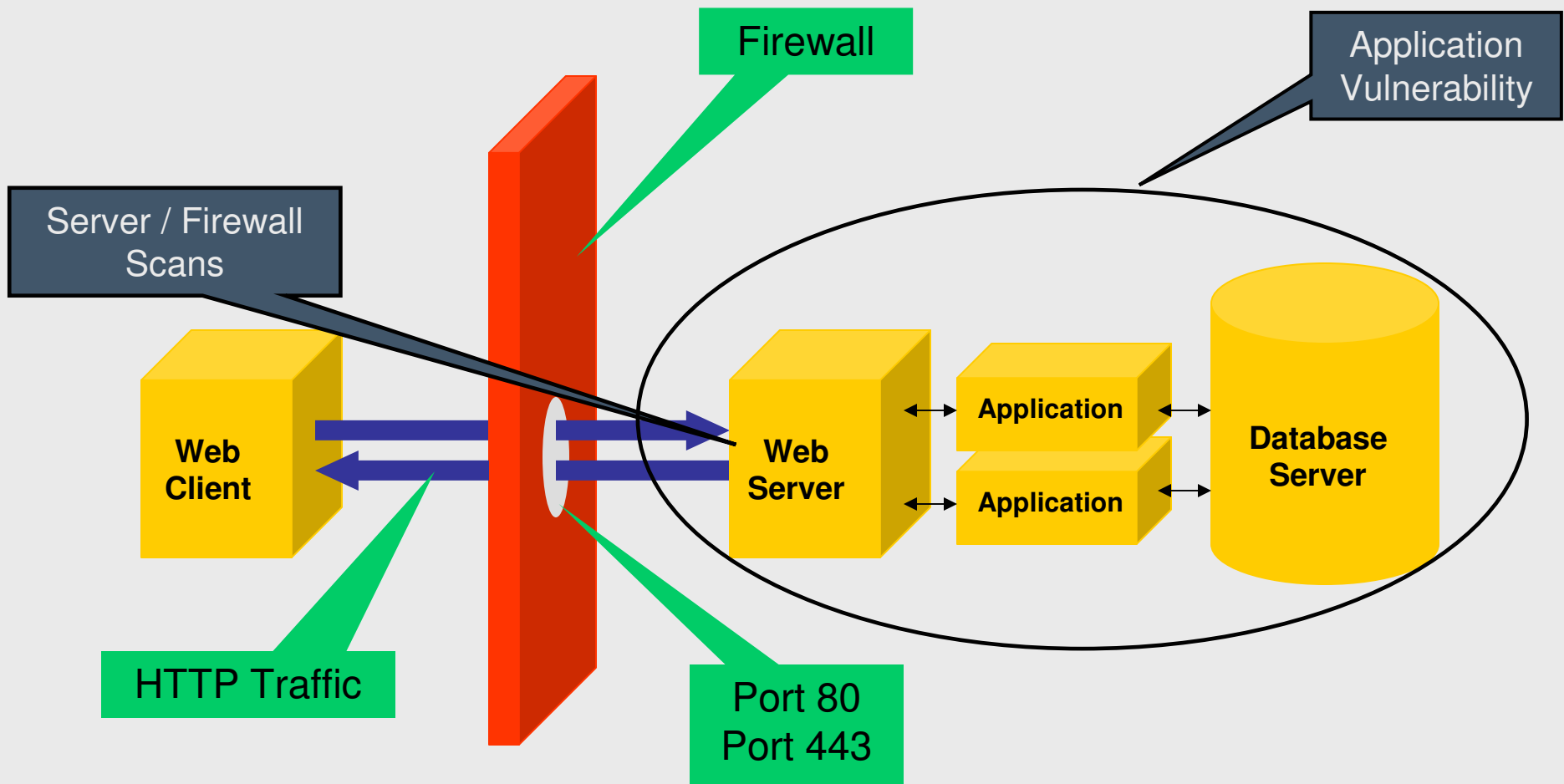
WWW.SECURITYCOMPASS.COM

Nish Bhalla, Founder, Security Compass

- OWASP, Toronto Chapter Leader
- Over 10 years industry experience
- “Buffer Overflow Attacks: Detect, Exploit & Prevent” and is a contributing author for “Windows XP Professional Security”, “HackNotes: Network Security” and “Hacking Exposed: Web Applications – 2nd”.
- Speaker : "Reverse Engineering Conference" in Montreal, "HackInTheBox" in Malaysia and "ISC2 Security" Conference in Las Vegas, New York etc.
- Developer and Trainer of security courses at Security Compass and Foundstone.
- Brining field work done for various fortune 500 and large software houses into class rooms.



Web Architecture



Original from <http://www.thinkingstone.com/talks/> by Ivan Ristic



Web Server

➤ Web Server Scans

- Full TCP / UDP Port Scans
- Web Server Scans
 - ▶ Nikto (www.cirt.net)
 - ▶ Spike Web Proxy (www.immunitysec.com)
 - ▶ Stealth Scanner (www.nstalker.com) Free / Commercial
- SSL Version (40/56/128 Bit)
- Administrator Port
- Reverse Proxy
- Internal IP
- Internal Port
- Internal Server Name
- Load Balancer



Web Applications

WWW.SECURITYCOMPASS.COM

- Web Application: Background Information on the site
 - Identify Technologies used and Application Architecture
 - Mirror site
 - Sift through client side code (review comments and client side code)
 - Authenticate to the site and browse the site
 - Document all the links and pages on the site

- Web Applications: Threat Analysis



Web Applications

- Web Application: Begin Testing of the Web Application
 - Configuration Management (Web Server)
 - Backup Files (.bak /.inc/.gz /.zip)
 - Authentication (Type of Authentication / Preventing Brute Force)
 - Authorization (ACLs on Files / ACLs on Data / Cookies)
 - Session / Cookie Management
 - Input Validation (XSS/SQL Injection/ Field Overflows/Field Underflow)
 - Hidden Tags / Hidden Cookie variables / Hidden Pages
 - File Upload (File Type / Location of upload)
 - Buffer Overflows (ISAPI/Modules)
 - Cryptography
 - Sensitive Data

- Web Application: Search Engine Hacking
 - groups.google.com
 - yahoo.com
 - archive.org



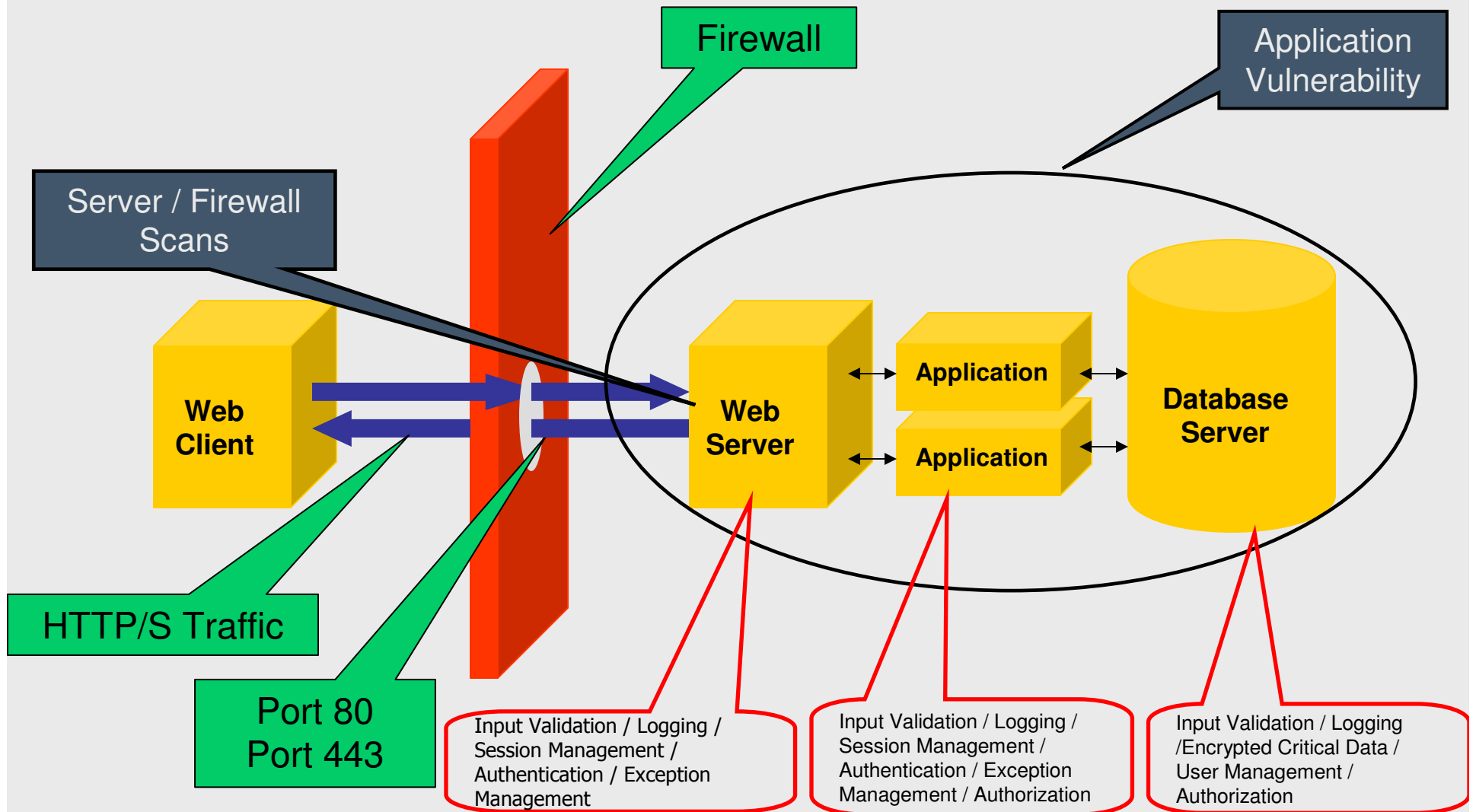
Application Architecture Components

WWW.SECURITYCOMPASS.COM

- Authentication
- Authorization
- Session Management
- User Management
- Cryptography, PII, Critical Data
- Data Validation
- Data Handling
- Error & Exception
- Event Logging



Architecture Map



Contact

WWW.SECURITYCOMPASS.COM

Nish[at]SecurityCompass(dot)com

